

Siber Zorbalığa Karşı Gençlik İttifakı



Politika Önerileri Raporu

"Avrupa Dayanışma Programı kapsamında Avrupa Birliği tarafından desteklenmektedir. Bu raporda yer alan görüş, değerlendirme ve öneriler yalnızca yazarlarına aittir. Avrupa Komisyonu ve Türkiye Ulusal Ajansı, bu yayında yer alan bilgilerin kullanımından veya içerdiği görüşlerden sorumlu tutulamaz."



**Avrupa Birliği tarafından
finanse edilmektedir**



2024-3-TR01-ESC30-SOL-000284071



**Avrupa Birliği tarafından
finanse edilmektedir**

ESC-30

Avrupa Dayanışma Programı Dayanışma Programı

Siber Zorbalığa Karşı Gençlik İttifakı

Politika Önerileri Raporu

SAKARYA ÜNİVERSİTESİ

Proje Ekibi

- Kayra Kaan KABAKÇIOĞLU
- Gülbin ABATAY
- Samet AYAN
- Yaren ŞÜKRE
- Ömer Faruk ACAR

Proje Koordinatörü

- Yusuf Buğra KILIÇ

Proje Koçu

- Öğr.Gör.Dr. Sadık DEMİRBAĞ

Politika Önerileri Mentörü

- Dr. Öğr. Üyesi Hatice TURUT DEMİRBAĞ



**Avrupa Birliği tarafından
finanse edilmektedir**



2024-3-TR01-ESC30-SOL-000284071



**Avrupa Birliği tarafından
finanse edilmektedir**

İÇİNDEKİLER

1.Giriş.....	9
2.Siber Zorbalık ve Mevcut Durum.....	11
2.1 Siber Zorbalığın Günümüzdeki Görünümü.....	11
2.2 Gençlerin Karşılaştığı Temel Sorunlar.....	12
2.3 Kurumsal ve Politik Düzeyde İhtiyaçlar.....	12
2.4 Politika Geliştirme İhtiyacı.....	13
3.Projenin Kapsamı ve Yöntemi.....	14
4.Bulgular ve Değerlendirme.....	18
4.1 Katılımcı Profili.....	18
4.2 Siber Zorbalık Farkındalığı.....	19
4.3 Dijital Haklar ve Güvenlik Bilinci.....	20
4.4 Proje Faaliyetlerinin Bilgi ve Farkındalık Üzerindeki Etkisi.....	21
4.5 Siber Zorbalık Karşısında Davranış Eğilimleri.....	22
4.6 Proje Faaliyetlerinin Değerlendirilmesi.....	24



**Avrupa Birliği tarafından
finanse edilmektedir**

5. Politika Önerileri.....	26
5.1 Siber Zorbalıkla Mücadelede Hukuki ve Kurumsal Yaptırımların Güçlendirilmesi.....	26
5.2 Eğitim ve Farkındalık Faaliyetlerinin Kurumsal Bir Yapıya Kavuşturulması.....	28
5.3 Sosyal Medya Platformlarında Önleyici Mekanizmaların Güçlendirilmesi.....	30
5.4 Üniversitelerde Siber Zorbalık Destek ve Başvuru Mekanizmalarının Güçlendirilmesi.....	31
5.5 Ulusal Düzeyde Kurumsal Koordinasyon ve Çok Paydaşlı İş Birliğinin Güçlendirilmesi.....	34
5.6 Sosyal Medya Platformlarında Hesap Verebilirlik ve Güvenli Dijital Ortamların Güçlendirilmesi.....	36
5.7 Sürekli İzleme, Araştırma ve Veri Temelli Politika Geliştirme Mekanizmalarının Oluşturulması.....	38
6.Sonuç ve Değerlendirme.....	41
6.1 Dijital Şiddet ve Türkiye’de Durum.....	42
6.2 Geleceğe Yönelik Perspektif.....	43
7. Yararlanılan Kaynaklar.....	45
8.Teşekkür.....	46



**Avrupa Birliği tarafından
finanse edilmektedir**

ÖZET

Siber Zorbalığa Karşı Gençlik İttifakı projesi, Avrupa Dayanışma Programı ESC30-SOL kapsamında Sakarya Üniversitesi öğrencilerinin koordinasyonunda yürütülen bir gençlik dayanışma projesidir. Proje, 18–30 yaş arası gençlerin dijital ortamlarda karşılaşılabilecekleri siber zorbalık, dijital şiddet, çevrimiçi taciz, kişisel verilerin ihlali ve güvenli internet kullanımı gibi konularda farkındalıklarını artırmayı amaçlamıştır.

Proje sürecinde gençlerin dijital dünyada daha güvenli, bilinçli ve sorumlu bireyler olarak yer almalarına katkı sağlanmış; özellikle üniversite öğrencilerinin siber zorbalığı tanıma, önleme ve karşılaştıkları durumlarda doğru destek mekanizmalarına başvuru kapasitelerinin güçlendirilmesi hedeflenmiştir. Bunun yanında, kadınlara yönelik dijital şiddet ve cinsiyet temelli siber zorbalık konusu proje kapsamında özel bir odak alanı olarak ele alınmıştır.

Proje kapsamında Sakarya Üniversitesi başta olmak üzere farklı yükseköğretim kurumlarında farkındalık faaliyetleri, eğitimler, seminerler, dijital içerik çalışmaları ve yaygınlaştırma faaliyetleri gerçekleştirilmiştir. Bu çalışmalar aracılığıyla gençlerin dijital güvenlik, dijital haklar, çevrimiçi riskler, siber suçlar ve güvenli dijital davranışlar konularında bilgi düzeylerinin artırılması amaçlanmıştır.

Bu politika önerileri raporu, proje süresince yürütülen faaliyetlerden, gençlerden alınan geri bildirimlerden, saha gözlemlerinden ve proje deneyimlerinden hareketle hazırlanmıştır. Rapor, siber zorbalıkla mücadelede yalnızca bireysel farkındalığın değil; aynı zamanda üniversiteler, kamu kurumları, yerel yönetimler, sivil toplum kuruluşları ve dijital platformlar düzeyinde kurumsal mekanizmaların geliştirilmesi gerektiğini ortaya koymaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Raporda; üniversitelerde dijital güvenlik eğitimlerinin yaygınlaştırılması, siber zorbalık bildirim ve destek mekanizmalarının güçlendirilmesi, psikolojik danışmanlık birimlerinin dijital şiddet konusunda kapasitesinin artırılması, gençlere yönelik erişilebilir bilgilendirme materyallerinin hazırlanması, kadınlara yönelik dijital şiddetle mücadeleyle özel destek modellerinin geliştirilmesi ve kurumlar arası iş birliğinin artırılması yönünde politika önerileri sunulmaktadır.

Bu raporun, gençlerin dijital dünyada daha güvenli, bilinçli ve destekleyici bir ortamda yer almasına katkı sağlaması ve siber zorbalıkla mücadelede karar alıcı kurumlar için yol gösterici bir kaynak olması hedeflenmektedir.

Proje Ekibi

Siber Zorbalığa Karşı Gençlik İttifakı



**Avrupa Birliği tarafından
finanse edilmektedir**

1. Giriş

Dijital teknolojilerin hızla gelişmesi ve çevrimiçi platformların günlük yaşamın ayrılmaz bir parçası hâline gelmesi, bireylere iletişim, eğitim ve bilgiye erişim açısından önemli fırsatlar sunarken; siber zorbalık, dijital şiddet, çevrimiçi taciz, kişisel verilerin kötüye kullanılması ve nefret söylemi gibi yeni risk alanlarını da beraberinde getirmiştir. Özellikle dijital ortamların en yoğun kullanıcıları arasında yer alan gençler, bu risklerden doğrudan etkilenen grupların başında gelmektedir.

Siber zorbalık, bireylerin bilgi ve iletişim teknolojileri aracılığıyla kasıtlı olarak tehdit edilmesi, aşağılanması, dışlanması veya psikolojik zarara uğratılması şeklinde ortaya çıkan çok boyutlu bir sorundur. Çevrimiçi ortamların anonim yapısı, içeriklerin hızla yayılabilmesi ve dijital izlerin kalıcılığı nedeniyle siber zorbalığın etkileri, geleneksel zorbalığa kıyasla daha geniş kitlelere ulaşabilmekte ve mağdurlar üzerinde uzun süreli sosyal, psikolojik ve akademik sonuçlar doğurabilmektedir.

Bu nedenle, siber zorbalıkla mücadele yalnızca bireysel farkındalık çalışmalarıyla sınırlı kalmamalı; eğitim kurumları, kamu kuruluşları, yerel yönetimler, sivil toplum kuruluşları ve dijital platformların ortak sorumluluk üstlendiği bütüncül politika yaklaşımlarıyla ele alınmalıdır. Dijital okuryazarlığın geliştirilmesi, güvenli dijital davranışların yaygınlaştırılması, etkili başvuru mekanizmalarının oluşturulması ve gençlerin karar alma süreçlerine katılımının desteklenmesi, sürdürülebilir çözümlerin temel unsurları arasında yer almaktadır.

Bu anlayış doğrultusunda Avrupa Dayanışma Programı (European Solidarity Corps – ESC30-SOL) kapsamında yürütülen **Siber Zorbalığa Karşı Gençlik İttifakı** projesi hayata geçirilmiştir. Proje kapsamında Sakarya Üniversitesi koordinasyonunda, farklı disiplinlerden gençlerin aktif katılımıyla dijital güvenlik



**Avrupa Birliği tarafından
finanse edilmektedir**

ve siber zorbalık konularında farkındalık faaliyetleri yürütülmüş; eğitimler, seminerler, kamu spotları, dijital içerikler ve yaygınlaştırma çalışmaları gerçekleştirilmiştir. Ayrıca üniversitelerde düzenlenen etkinlikler ve katılımcılardan elde edilen geri bildirimler doğrultusunda siber zorbalıkla mücadeleye yönelik politika geliştirme süreci yürütülmüştür.

Bu politika önerileri raporu, proje boyunca edinilen deneyimler, gerçekleştirilen faaliyetler, katılımcı görüşleri ve saha gözlemlerinden elde edilen bulgular temel alınarak hazırlanmıştır. Raporun amacı; siber zorbalıkla mücadelede mevcut ihtiyaçları ortaya koymak, gençlerin beklenti ve önerilerini değerlendirmek ve başta kamu kurumları, yükseköğretim kurumları, yerel yönetimler ve sivil toplum kuruluşları olmak üzere ilgili paydaşlar için uygulanabilir, sürdürülebilir ve kanıta dayalı politika önerileri sunmaktır.



**Avrupa Birliği tarafından
finanse edilmektedir**

2.Siber Zorbalık ve Mevcut Durum

Siber zorbalık, dijital teknolojilerin yaygınlaşmasıyla birlikte bireysel bir sorun olmanın ötesine geçerek eğitim, psikoloji, hukuk, bilgi güvenliği ve insan hakları gibi birçok alanı ilgilendiren çok boyutlu bir toplumsal mesele hâline gelmiştir. Etkili politika önerileri geliştirebilmek için öncelikle mevcut durumun, gençlerin karşılaştığı temel sorunların ve bu sorunların kurumsal düzeyde nasıl ele alındığının değerlendirilmesi gerekmektedir. Bu bölümde, siber zorbalığın güncel görünümü, gençler üzerindeki etkileri ve politika geliştirilmesini gerekli kılan temel ihtiyaç alanları ele alınmaktadır.

2.1 Siber Zorbalığın Günümüzdeki Görünümü

Dijitalleşmenin hız kazanmasıyla birlikte internet ve sosyal medya platformları, bireylerin günlük yaşamında vazgeçilmez iletişim araçları hâline gelmiştir. Özellikle gençler eğitim, sosyal etkileşim, eğlence ve bilgiye erişim süreçlerinde çevrimiçi ortamları yoğun olarak kullanmaktadır. Bu durum dijital dünyanın sunduğu fırsatları artırırken, bireylerin çevrimiçi risklerle karşılaşma olasılığını da yükseltmektedir.

Bu risklerin başında gelen siber zorbalık; sosyal medya, mesajlaşma uygulamaları, çevrimiçi oyun platformları, forumlar ve diğer dijital iletişim araçları üzerinden gerçekleştirilen hakaret, tehdit, aşağılama, dışlama, ifşa, kimlik taklidi ve benzeri zarar verici davranışları kapsamaktadır. Dijital içeriklerin hızlı yayılması, anonim hesapların kullanılabilmesi ve içeriklerin uzun süre erişilebilir kalması, siber zorbalığın etkilerini geleneksel zorbalığa kıyasla daha karmaşık ve kalıcı hâle getirmektedir.

Araştırmalar, gençlerin önemli bir bölümünün yaşamlarının herhangi bir döneminde siber zorbalığa maruz kaldığını veya siber zorbalık davranışlarına tanıklık ettiğini göstermektedir. Buna rağmen mağdurların önemli bir kısmı yaşadıkları olayları resmi kurumlara veya eğitim kurumlarına bildirmemekte, çözümü çoğu zaman bireysel yöntemlerle aramaktadır. Bu durum hem olayların



**Avrupa Birliği tarafından
finanse edilmektedir**

görünürlüğünü azaltmakta hem de etkili müdahale mekanizmalarının geliştirilmesini zorlaştırmaktadır.

2.2 Gençlerin Karşılaştığı Temel Sorunlar

Proje kapsamında gerçekleştirilen faaliyetler, eğitimler ve katılımcılarla yapılan etkileşimler sonucunda gençlerin siber zorbalık konusunda benzer sorunlarla karşı karşıya olduğu gözlemlenmiştir.

Bunların başında siber zorbalığın kapsamının yeterince bilinmemesi gelmektedir. Birçok genç yalnızca açık hakaret veya tehdit içerikli davranışları siber zorbalık olarak değerlendirirken; dijital dışlama, izinsiz içerik paylaşımı, manipülasyon, sahte hesap oluşturma veya sürekli rahatsız etme gibi davranışların da siber zorbalık kapsamında değerlendirilebileceğinin farkında değildir.

Bunun yanında gençlerin önemli bir kısmı karşılaştıkları olaylarda hangi kuruma başvurabileceklerini, hangi hukuki haklara sahip olduklarını ve hangi dijital platformların hangi başvuru mekanizmalarını sunduğunu yeterince bilmemektedir. Bu durum mağdurların destek mekanizmalarına erişimini güçleştirmektedir.

Bir diğer önemli sorun ise dijital güvenlik farkındalığındaki eksikliktir. Güçlü parola kullanımı, iki aşamalı kimlik doğrulama, kişisel verilerin korunması, gizlilik ayarlarının doğru yapılandırılması ve dijital ayak izi gibi temel dijital güvenlik uygulamaları konusunda bilgi düzeylerinin farklılık gösterdiği gözlemlenmiştir.

2.3 Kurumsal ve Politik Düzeyde İhtiyaçlar

Siber zorbalık yalnızca bireysel davranışlardan kaynaklanan bir problem değildir. Eğitim kurumları, kamu kurumları, yerel yönetimler, dijital platformlar ve sivil toplum kuruluşlarının koordineli çalışmasını gerektiren çok paydaşlı bir politika alanıdır.

Üniversitelerde siber zorbalığa ilişkin standart başvuru mekanizmalarının bulunmaması, öğrencilerin konuya ilişkin düzenli eğitimlere erişememesi ve



**Avrupa Birliği tarafından
finanse edilmektedir**

psikososyal destek hizmetlerinin dijital şiddet boyutunu yeterince kapsayamaması, kurumsal kapasitenin geliştirilmesi gereken alanlar arasında yer almaktadır.

Bununla birlikte dijital platformların içerik moderasyonu, şikâyet süreçlerinin erişilebilirliği ve kullanıcıların hak arama mekanizmalarına ilişkin bilgilendirilmesi konularında da geliştirilmesi gereken yönler bulunmaktadır. Gençlerin güvenli dijital ortamlarda bulunabilmesi için yalnızca bireysel farkındalığın artırılması değil, kurumlar arası iş birliğini güçlendiren ve önleyici politikaları esas alan bütüncül yaklaşımların benimsenmesi gerekmektedir.

2.4 Politika Geliştirme İhtiyacı

Siber zorbalığın sürekli değişen dijital ortamlarla birlikte yeni biçimler kazanması, bu alanda geliştirilecek politikaların da dinamik ve sürdürülebilir olmasını zorunlu kılmaktadır. Gençlerin deneyimlerini merkeze alan, eğitim ve farkındalık faaliyetlerini kurumsal mekanizmalarla destekleyen, dijital haklar ve güvenli internet kullanımını bütüncül şekilde ele alan politika yaklaşımları, uzun vadeli çözümler açısından büyük önem taşımaktadır.

Bu raporda sunulan politika önerileri, proje kapsamında yürütülen faaliyetlerden, katılımcı geri bildirimlerinden ve saha deneyimlerinden hareketle hazırlanmış olup; siber zorbalıkla mücadelede uygulanabilir, genç odaklı ve kurumlar arası iş birliğini güçlendirmeyi hedefleyen öneriler ortaya koymayı amaçlamaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

3.Projenin Kapsamı ve Yöntemi

Avrupa Dayanışma Programı (European Solidarity Corps – ESC30-SOL) kapsamında desteklenen Siber Zorbalığa Karşı Gençlik İttifakı projesi, dijitalleşmenin gençlerin günlük yaşamındaki etkisinin giderek artmasıyla birlikte yaygınlaşan siber zorbalık, dijital şiddet, çevrimiçi taciz, dolandırıcılık, şantaj, kişisel verilerin ihlali ve diğer dijital güvenlik risklerine karşı gençlerin bilinç düzeyini artırmak amacıyla geliştirilmiştir. Proje, yalnızca bireysel farkındalık oluşturmayı değil, aynı zamanda gençlerin dijital haklarını bilen, güvenli dijital davranışlar geliştiren ve karşılaştıkları çevrimiçi riskler karşısında doğru destek mekanizmalarına başvurabilen aktif dijital vatandaşlar hâline gelmelerini hedeflemiştir.

Proje, Sakarya Üniversitesi öğrencilerinin koordinasyonunda ve farklı disiplinlerden oluşan genç bir ekip tarafından yürütülmüştür. Yazılım mühendisliği, bilgisayar mühendisliği, sosyoloji, coğrafya, iktisat ve matematik gibi farklı alanlardan gelen ekip üyeleri, siber zorbalık sorununu yalnızca teknik değil; sosyal, psikolojik, hukuki ve eğitsel boyutlarıyla ele almıştır. Bu disiplinler arası yaklaşım, proje faaliyetlerinin planlanması ve politika önerilerinin geliştirilmesi sürecinde bütüncül bir bakış açısı kazandırmıştır.

Projenin hedef kitlesini, dijital teknolojileri aktif olarak kullanan 18–30 yaş arasındaki gençler, özellikle üniversite öğrencileri oluşturmuştur. Bunun yanında öğretim elemanları, gençlik çalışanları, sivil toplum kuruluşları ve ilgili kamu kurumlarının temsilcileri de proje faaliyetlerine dolaylı olarak dâhil edilerek çok



**Avrupa Birliği tarafından
finanse edilmektedir**

paydaşlı bir iş birliği modeli benimsenmiştir. Projede özellikle kadınların dijital ortamlarda maruz kaldığı çevrimiçi şiddet ve cinsiyet temelli siber zorbalık konuları da öncelikli çalışma alanları arasında değerlendirilmiştir.

Proje uygulama süreci, başvuru aşamasında belirlenen faaliyet planına uygun olarak yürütülmüş ve büyük ölçüde planlanan çıktılara ulaşılmıştır. Bu kapsamda Sakarya Üniversitesi, Kocaeli Üniversitesi, Düzce Üniversitesi, Bursa Uludağ Üniversitesi, Marmara Üniversitesi ve Sakarya Uygulamalı Bilimler Üniversitesinde siber zorbalık ve dijital güvenlik temalı seminerler ve farkındalık etkinlikleri düzenlenmiştir. Etkinliklerde gençlere; siber zorbalığın tanımı, türleri, psikolojik etkileri, hukuki boyutu, kişisel verilerin korunması, dijital mahremiyet, güvenli sosyal medya kullanımı ve çevrimiçi tehditlere karşı alınabilecek önlemler hakkında uygulamalı eğitimler verilmiştir.

Yüz yüze gerçekleştirilen faaliyetlerin yanı sıra projenin etkisinin daha geniş kitlelere ulaştırılabilmesi amacıyla kapsamlı bir dijital yaygınlaştırma stratejisi uygulanmıştır. Proje için kurumsal kimlik oluşturulmuş, sosyal medya hesapları açılmış ve proje faaliyetlerinin sürdürülebilir şekilde paylaşılacağı bir web sitesi kurulmuştur. Eğitim içerikleri, bilgilendirici görseller, kısa videolar ve farkındalık mesajları düzenli olarak dijital platformlarda yayımlanmış; böylece yalnızca etkinliklere katılan gençlere değil, çevrimiçi ortamda projeyi takip eden çok daha geniş bir hedef kitleye erişim sağlanmıştır.

Toplumsal farkındalığın artırılması amacıyla proje kapsamında dört kamu spotu hazırlanmış ve bu içerikler üniversitelerde gerçekleştirilen etkinliklerde, proje web



**Avrupa Birliği tarafından
finanse edilmektedir**

sitesinde ve sosyal medya platformlarında yayımlanmıştır. Kamu spotlarında güvenli internet kullanımı, siber zorbalığın erken fark edilmesi, dijital hakların korunması ve çevrimiçi ortamda saygılı iletişim kültürünün geliştirilmesi gibi temel mesajlara yer verilmiştir. Böylece siber zorbalık konusunda yalnızca bilgi aktarımı yapılmamış, aynı zamanda davranış değişikliği oluşturmayı hedefleyen iletişim faaliyetleri de yürütülmüştür.

Proje süresince kamu kurumları, akademisyenler ve ilgili paydaşlarla iş birlikleri geliştirilmiş; gençlerin ihtiyaç ve beklentilerini daha doğru analiz edebilmek amacıyla katılımcı geri bildirimleri sistematik biçimde değerlendirilmiştir. Eğitim faaliyetleri sonrasında katılımcılardan alınan değerlendirmeler, etkinlik gözlemleri ve proje ekibinin saha deneyimleri analiz edilerek ortak eğilimler belirlenmiştir. Elde edilen bulgular, yalnızca proje çıktılarının değerlendirilmesinde değil, aynı zamanda bu raporda sunulan politika önerilerinin oluşturulmasında da temel veri kaynaklarından biri olarak kullanılmıştır.

Politika önerilerinin hazırlanması sürecinde yalnızca proje kapsamında elde edilen verilerle yetinilmemiş; Avrupa Birliği'nin dijital güvenlik politikaları, Avrupa Birliği Siber Güvenlik Ajansı (ENISA) tarafından yayımlanan rehberler, ulusal mevzuat, akademik çalışmalar ve uluslararası iyi uygulama örnekleri de incelenmiştir. Bu çok kaynaklı yaklaşım sayesinde proje deneyimleri bilimsel literatür ve mevcut politika belgeleriyle birlikte değerlendirilmiş, önerilerin uygulanabilirliği ve sürdürülebilirliği güçlendirilmiştir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Hazırlanan politika önerileri, proje sonunda sistematik biçimde analiz edilerek ilgili karar alıcı kurumlarla paylaşılmak üzere derlenmiştir. Böylece proje yalnızca farkındalık oluşturan bir gençlik girişimi olmanın ötesine geçmiş; gençlerin görüşlerini politika geliştirme süreçlerine taşıyan, katılımcı ve kanıta dayalı bir model ortaya koymuştur. Bu rapor, proje sürecinde elde edilen deneyimlerin kalıcı ve uygulanabilir politika önerilerine dönüştürülmesini amaçlayan temel çıktılardan biri niteliğindedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

4.Bulgular ve Değerlendirme

Bu bölümde, **Siber Zorbalığa Karşı Gençlik İttifakı** projesi kapsamında gerçekleştirilen farkındalık etkinlikleri sonrasında uygulanan anketten elde edilen bulgular değerlendirilmiştir. Anket, katılımcıların siber zorbalık, dijital güvenlik, dijital haklar, çevrimiçi riskler, kadınlar için dijital güvenlik ve etkinlik değerlendirmelerine ilişkin algılarını ölçmeyi amaçlamıştır.

Veriler, nicel ve nitel değerlendirme yaklaşımıyla ele alınmıştır. Nicel bölümde katılımcıların 1–5 aralığında verdikleri yanıtlar analiz edilmiş; 4 ve 5 puanlar olumlu/kabul düzeyi yüksek yanıtlar olarak değerlendirilmiştir. Nitel bölümde ise katılımcıların açık uçlu politika önerileri tematik olarak incelenmiş ve tekrar eden öneri alanları belirlenmiştir.

4.1 Katılımcı Profili

Ankete toplam 228 kişi katılım sağlamıştır. Katılımcıların cinsiyet dağılımı dengeli bir yapı göstermektedir. Katılımcıların 118'i kadın, 110'u erkektir. Bu dağılım, proje kapsamında elde edilen verilerin hem kadın hem erkek gençlerin görüşlerini içerecek şekilde dengeli bir katılımcı profiline dayandığını göstermektedir.

Yaş dağılımı incelendiğinde katılımcıların büyük çoğunluğunun gençlerden oluştuğu görülmektedir. Katılımcıların önemli bölümü 18–23 yaş aralığında yer almakta olup, medyan yaş 20 olarak hesaplanmıştır. Bu durum, projenin hedef kitlesi olan gençlere ve özellikle üniversite öğrencilerine doğrudan ulaştığını göstermektedir.

Katılımcılar farklı üniversitelerden ankete dâhil olmuştur. Verilerde Sakarya Üniversitesi, Sakarya Uygulamalı Bilimler Üniversitesi, Düzce Üniversitesi, Kocaeli Üniversitesi, Bursa Uludağ Üniversitesi ve Marmara Üniversitesi gibi farklı yükseköğretim kurumlarından yanıtlar yer almaktadır. Bu çeşitlilik, projenin tek bir kampüsle sınırlı kalmadığını; farklı üniversite ortamlarında gençlerin siber



**Avrupa Birliği tarafından
finanse edilmektedir**

zorbalık ve dijital güvenlik konularına ilişkin görüşlerinin toplandığını göstermektedir.

Katılımcı profili genel olarak değerlendirildiğinde, anket verilerinin proje hedef kitlesiyle uyumlu olduğu, üniversite gençliğinin dijital güvenlik ve siber zorbalık konularındaki farkındalık düzeyini değerlendirmek için uygun bir örneklem sunduğu görülmektedir.

4.2 Siber Zorbalık Farkındalığı

Proje kapsamında uygulanan farkındalık anketi sonuçları, katılımcıların siber zorbalık konusunda genel olarak yüksek bir farkındalık düzeyine sahip olduğunu göstermektedir. “Siber zorbalığın ne olduğunu ve kapsamını biliyorum.” ifadesine katılımcıların **%90,35’i** “Katılıyorum” veya “Kesinlikle Katılıyorum” yanıtını vermiştir. Bu ifadeye ilişkin ortalama puan **4,44/5** olarak hesaplanmıştır.

Bu bulgu, proje kapsamında gerçekleştirilen seminerler, eğitim faaliyetleri ve farkındalık çalışmalarının katılımcıların siber zorbalık kavramını yalnızca tanımasına değil, aynı zamanda kapsamını doğru şekilde değerlendirebilmesine katkı sağladığını göstermektedir. Siber zorbalığın yalnızca hakaret veya tehdit gibi doğrudan saldırılarla sınırlı olmadığı; dijital dışlama, kimlik taklidi, izinsiz içerik paylaşımı, çevrimiçi taciz ve kişisel verilerin kötüye kullanılması gibi farklı davranış biçimlerini de kapsadığı yönündeki farkındalığın güçlendiği değerlendirilmektedir.

Bununla birlikte katılımcıların **%86,40’ı** siber zorbalığın bireysel ve toplumsal etkilerini anlayabildiğini belirtmiştir (Ortalama: **4,42/5**). Bu sonuç, gençlerin siber zorbalığın yalnızca mağduru değil; aileyi, eğitim ortamını, sosyal ilişkileri ve toplumdaki dijital güvenlik algısını da etkileyen çok boyutlu bir sorun olduğunun farkında olduklarını göstermektedir.

Anket sonuçları ayrıca katılımcıların **%88,16’sının** dijital ortamlarda karşılaşılan risk ve tehditleri tanıyabildiğini ortaya koymuştur (Ortalama: **4,36/5**). Bu durum,



**Avrupa Birliği tarafından
finanse edilmektedir**

proje faaliyetlerinde ele alınan dijital dolandırıcılık, kimlik avı (phishing), sahte hesaplar, zararlı bağlantılar ve kişisel veri güvenliği gibi konuların katılımcılar tarafından benimsendiğini göstermektedir.

Elde edilen bulgular genel olarak değerlendirildiğinde, proje faaliyetlerinin katılımcıların siber zorbalık ve dijital güvenlik konularındaki temel bilgi düzeylerini artırdığı ve gençlerde koruyucu dijital davranışların gelişmesine katkı sağladığı söylenebilir. Bununla birlikte farkındalığın kalıcı hâle getirilebilmesi için benzer eğitim ve bilinçlendirme faaliyetlerinin farklı üniversitelerde düzenli aralıklarla sürdürülmesi önem taşımaktadır.

4.3 Dijital Haklar ve Dijital Güvenlik Bilinci

Anket bulguları, katılımcıların siber zorbalık ve dijital güvenlik konusunda yüksek düzeyde farkındalık geliştirdiğini ortaya koyarken, dijital haklar konusunda bilgi düzeyinin diğer alanlara kıyasla daha düşük olduğunu göstermektedir. “Dijital haklarımın neler olduğunu biliyorum.” ifadesine katılımcıların **%62,28**’i “Katılıyorum” veya “Kesinlikle Katılıyorum” yanıtını vermiş, bu ifade için ortalama puan **3,82/5** olarak hesaplanmıştır. Araştırmada yer alan tüm değerlendirme maddeleri arasında bu ifade en düşük ortalama sahip bulgulardan biridir.

Bu sonuç, gençlerin siber zorbalığın ne olduğu konusunda farkındalık sahibi olmalarına rağmen, kişisel verilerin korunması, çevrimiçi mahremiyet, dijital platformlarda kullanıcı hakları, içerik kaldırma ve şikâyet mekanizmaları gibi dijital haklar alanında daha fazla bilgi ve yönlendirmeye ihtiyaç duyduklarını göstermektedir. Dolayısıyla siber zorbalıkla mücadelede yalnızca risklerin tanıtılması yeterli olmayıp, bireylerin sahip oldukları hakları ve bu hakları nasıl kullanabileceklerini de öğrenmeleri gerekmektedir.

Öte yandan, “Kadınlar için dijital güvenliğin neden özel önem taşıdığını biliyorum.” ifadesine katılımcıların **%92,98**’i olumlu yanıt vermiş, bu ifade **4,61/5** ortalama ile araştırmadaki en yüksek değerlendirme puanına ulaşmıştır. Bu bulgu,



**Avrupa Birliği tarafından
finanse edilmektedir**

proje kapsamında kadınlara yönelik dijital şiddet, çevrimiçi taciz ve toplumsal cinsiyet temelli dijital risklere ilişkin yürütülen bilgilendirme çalışmalarının katılımcılar üzerinde güçlü bir farkındalık oluşturduğunu göstermektedir.

Elde edilen sonuçlar birlikte değerlendirildiğinde, katılımcılar siber zorbalığın etkileri ve dijital güvenliğin önemi konusunda yüksek bilinç düzeyine sahip olmakla birlikte, bu farkındalığın hukuki ve kurumsal boyutunu oluşturan dijital haklar konusunda desteklenmesi gerektiği görülmektedir. Bu nedenle üniversitelerde ve gençlik çalışmalarında dijital haklar, kişisel verilerin korunması, çevrimiçi başvuru mekanizmaları ve güvenli internet kullanımı konularını kapsayan uygulamalı eğitimlerin yaygınlaştırılması önem taşımaktadır.

Bu bulgu, raporun ilerleyen bölümlerinde sunulan dijital haklar eğitimlerinin yaygınlaştırılması, üniversitelerde dijital danışmanlık mekanizmalarının oluşturulması ve gençlere yönelik erişilebilir rehber materyaller hazırlanması yönündeki politika önerilerinin temel dayanaklarından birini oluşturmaktadır.

4.4 Proje Faaliyetlerinin Bilgi ve Farkındalık Üzerindeki Etkisi

Proje kapsamında gerçekleştirilen eğitimler, seminerler ve farkındalık etkinliklerinin katılımcılar üzerindeki etkisi, anket sonuçları doğrultusunda değerlendirilmiştir. Bulgular, faaliyetlerin yalnızca bilgi aktarımıyla sınırlı kalmadığını; aynı zamanda katılımcıların dijital güvenlik, siber zorbalık ve güvenli internet kullanımı konularındaki farkındalık düzeylerini artırdığını göstermektedir.

Anket sonuçlarına göre katılımcıların **%91,67'si** proje kapsamında gerçekleştirilen eğitimlerin siber zorbalık konusunda bilgi düzeylerini artırdığını belirtmiştir. Bu ifadeye verilen yanıtların ortalaması **4,56/5** olarak hesaplanmıştır. Elde edilen bu sonuç, proje kapsamında uygulanan eğitim içeriklerinin hedef kitlenin ihtiyaçlarına uygun şekilde planlandığını ve öğrenme çıktılarının büyük ölçüde karşılandığını göstermektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Benzer şekilde katılımcıların büyük çoğunluğu, proje faaliyetlerinin dijital ortamda daha güvenli davranışlar geliştirmelerine katkı sağladığını ifade etmiştir. Eğitimlerde ele alınan güçlü parola kullanımı, iki aşamalı kimlik doğrulama, kişisel verilerin korunması, sosyal medya gizlilik ayarları ve güvenli dijital iletişim gibi konuların katılımcılar tarafından günlük yaşamlarında uygulanabilir bilgiler olarak değerlendirildiği görülmüştür.

Katılımcı değerlendirmeleri, proje faaliyetlerinin yalnızca teorik bilgi sunmakla kalmadığını; gerçek yaşam örnekleri, vaka analizleri ve etkileşimli anlatım yöntemleri sayesinde öğrenme sürecini desteklediğini ortaya koymaktadır. Bu durum, gençlerin siber zorbalıkla karşılaşmaları hâlinde nasıl hareket etmeleri gerektiği konusunda daha bilinçli karar verebilmelerine katkı sağlamaktadır.

Ayrıca proje süresince gerçekleştirilen seminerler, kamu spotları, dijital içerikler ve sosyal medya paylaşımları sayesinde farkındalık çalışmalarının yalnızca etkinliklere katılan bireylerle sınırlı kalmadığı; çevrimiçi ortamlar aracılığıyla daha geniş kitlelere ulaştığı değerlendirilmektedir. Böylece proje, yüz yüze eğitim faaliyetleri ile dijital yaygınlaştırma çalışmalarını bir araya getirerek çok yönlü bir farkındalık modeli ortaya koymuştur.

Bu bulgular, gençlere yönelik siber zorbalık eğitimlerinin kısa süreli farkındalık faaliyetleri olarak değil, yükseköğretim kurumlarında ve gençlik çalışmalarında sürdürülebilir eğitim programları hâline getirilmesinin önemini ortaya koymaktadır. Proje kapsamında elde edilen olumlu sonuçlar, benzer eğitim modellerinin farklı üniversitelerde ve gençlik merkezlerinde yaygınlaştırılmasının siber zorbalıkla mücadelede önemli katkılar sağlayacağını göstermektedir.

4.5 Siber Zorbalık Karşısında Davranış Eğilimleri

Siber zorbalıkla mücadelede farkındalık kadar, bireylerin karşılaştıkları durumlarda nasıl hareket edeceklerini bilmeleri de büyük önem taşımaktadır. Bu nedenle anket



**Avrupa Birliği tarafından
finanse edilmektedir**

kapsamında katılımcıların siber zorbalık karşısındaki tutum ve davranış eğilimleri değerlendirilmiştir.

Anket sonuçlarına göre katılımcıların **%82,02'si** siber zorbalığa tanık olduklarında tepki göstermenin önemli olduğunu belirtmiştir. Bu ifadeye verilen yanıtların ortalaması **4,27/5** olarak hesaplanmıştır. Bu bulgu, katılımcıların önemli bir bölümünün siber zorbalığı yalnızca mağdurun değil, toplumun ortak sorumluluğu olarak değerlendirdiğini göstermektedir. Pasif izleyici davranışının azaltılması ve güvenli dijital ortamların oluşturulması açısından bu yaklaşım olumlu bir göstergedir.

Buna karşın, **“Siber zorbalığa uğrayan bir kişiye nasıl destek olacağımı biliyorum.”** ifadesinde olumlu yanıt oranı **%68,86**'da kalmış, ortalama puan ise **3,90/5** olarak hesaplanmıştır. Bu sonuç, katılımcıların siber zorbalığın yanlış bir davranış olduğu konusunda bilinçli olmalarına rağmen, mağdurlara nasıl destek olunacağı konusunda bilgi ve beceri eksikliği yaşayabildiklerini göstermektedir.

Benzer şekilde, **%75,00** oranındaki katılımcı siber zorbalığın yetkili kişi veya kurumlara bildirilmesi gerektiğini ifade etmiş, bu maddeye ilişkin ortalama puan **4,17/5** olarak belirlenmiştir. Her ne kadar bu oran genel olarak olumlu kabul edilse de yaklaşık dört katılımcıdan birinin bildirim mekanizmaları konusunda yeterince güçlü bir tutum sergilememesi dikkat çekmektedir. Bu durum, gençlerin yalnızca farkındalık kazanmasının yeterli olmadığını; başvuru yolları, hukuki süreçler ve kurumsal destek mekanizmaları hakkında daha uygulamalı bilgilendirmeye ihtiyaç duyduklarını göstermektedir.

Bulgular birlikte değerlendirildiğinde, katılımcılar siber zorbalığın önlenmesi konusunda duyarlı bir yaklaşım sergilemekte; ancak mağdurlara destek olma yöntemleri ve resmî başvuru mekanizmalarının kullanımı konusunda geliştirilmesi gereken alanlar bulunmaktadır. Bu nedenle gelecekte yürütülecek farkındalık çalışmalarında yalnızca siber zorbalığın tanımı ve etkilerine değil, aynı zamanda **olay anında izlenecek adımlar, psikososyal destek kaynakları, hukuki haklar**



**Avrupa Birliği tarafından
finanse edilmektedir**

ve resmî bildirim süreçlerine ilişkin uygulamalı eğitim içeriklerine daha fazla yer verilmesi önem taşımaktadır.

4.6 Proje Faaliyetlerinin Değerlendirilmesi

Proje kapsamında gerçekleştirilen eğitimler, seminerler ve farkındalık faaliyetlerinin etkililiği, katılımcı memnuniyeti ve öğrenme kazanımları açısından değerlendirilmiştir. Anket bulguları, faaliyetlerin hem içerik kalitesi hem de uygulama yöntemi bakımından katılımcılar tarafından olumlu değerlendirildiğini göstermektedir.

Katılımcıların **%76,32'si**, proje kapsamında gerçekleştirilen sunum ve eğitimlerin konuları daha iyi anlamalarına katkı sağladığını belirtmiştir. Bu ifadeye verilen yanıtların ortalaması **4,22/5** olarak hesaplanmıştır. Bu bulgu, eğitim içeriklerinin hedef kitlenin bilgi düzeyi ve ihtiyaçları dikkate alınarak hazırlandığını ve öğrenme sürecini destekleyen etkili bir yöntem izlendiğini göstermektedir.

Eğitim faaliyetlerinin başarısında eğitici ve konuşmacıların bilgi birikimi de önemli bir unsur olarak öne çıkmıştır. Katılımcıların **%77,19'u**, konuşmacıların ele alınan konulara hâkim olduğunu ve içerikleri anlaşılır şekilde aktardığını ifade etmiş, bu madde **4,25/5** ortalama puan almıştır. Bu durum, proje kapsamında görev alan eğitimcilerin ve uzmanların güvenilir bilgi aktarımı sağladığını ve katılımcıların eğitim sürecine olan güvenini artırdığını göstermektedir.

Etkinliklerin organizasyon yapısına ilişkin değerlendirmeler de genel olarak olumlu sonuçlar ortaya koymuştur. Katılımcıların **%82,02'si**, etkinlik süresinin içerik aktarımı açısından yeterli olduğunu belirtmiştir. Ayrıca eğitimlerin planlanması, uygulama süreci ve katılımcılarla kurulan etkileşim de yüksek düzeyde memnuniyetle değerlendirilmiştir. Bu sonuçlar, proje faaliyetlerinin yalnızca içerik bakımından değil, organizasyonel açıdan da başarılı şekilde yürütüldüğünü göstermektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Anketin dikkat çekici bulgularından biri ise benzer faaliyetlerin yaygınlaştırılmasına yönelik güçlü taleptir. Katılımcıların **%86,84'ü**, siber zorbalık ve dijital güvenlik temalı eğitimlerin diğer üniversitelerde de düzenlenmesi gerektiğini ifade etmiştir. Bu bulgu, proje faaliyetlerinin katılımcılar tarafından yalnızca bireysel gelişim açısından değil, yükseköğretim kurumlarında yaygınlaştırılması gereken iyi bir uygulama modeli olarak değerlendirildiğini ortaya koymaktadır.

Genel değerlendirme sonuçları incelendiğinde, proje kapsamında uygulanan eğitim modelinin katılımcılar tarafından yüksek düzeyde kabul gördüğü ve hedef kitlenin ihtiyaçlarına cevap verebildiği anlaşılmaktadır. Bununla birlikte, siber zorbalıkla mücadelede tek seferlik eğitimlerin yeterli olmayacağı; dijital güvenlik ve dijital vatandaşlık konularının üniversitelerde süreklilik arz eden eğitim programları, oryantasyon faaliyetleri ve gençlik çalışmaları içerisine entegre edilmesinin daha kalıcı sonuçlar sağlayacağı değerlendirilmektedir.

Bu bulgular doğrultusunda, proje kapsamında geliştirilen eğitim modeli ve yaygınlaştırma yaklaşımının farklı yükseköğretim kurumlarında uygulanabilecek örnek bir model niteliği taşıdığı söylenebilir. Elde edilen sonuçlar, siber zorbalıkla mücadelede gençlerin aktif katılımını esas alan, uygulamalı öğrenmeyi destekleyen ve çok paydaşlı iş birliğini önceleyen yaklaşımların etkili olduğunu göstermektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

5. Politika Önerileri

Proje kapsamında katılımcılara yöneltilen “Eğer siz bir politika yapıcı olsaydınız, siber zorbalıkla mücadele için hangi önlemleri veya politika önerilerini geliştirirdiniz?” sorusuna verilen 228 açık uçlu yanıt içerik analizi yöntemiyle incelenmiştir. Yanıtlar benzer ifadeler doğrultusunda kodlanmış, ortak temalar belirlenmiş ve bu temalar ulusal ve uluslararası iyi uygulamalar ile birlikte değerlendirilmiştir. Analiz sonucunda katılımcı görüşlerinin altı temel politika alanında yoğunlaştığı görülmüştür. Bu bölümde sunulan öneriler, proje kapsamında elde edilen nicel bulgular, açık uçlu katılımcı görüşleri ve literatürde yer alan iyi uygulamalar birlikte değerlendirilerek hazırlanmıştır.

5.1 Siber Zorbalıkla Mücadelede Hukuki ve Kurumsal Yaptırımların Güçlendirilmesi

Sorunun Tanımı

İçerik analizi sonucunda katılımcılar tarafından en sık dile getirilen tema, siber zorbalık fiillerine yönelik **daha caydırıcı hukuki yaptırımların uygulanması** olmuştur. Açık uçlu yanıtlarda “cezaların ağırlaştırılması”, “hukuki yaptırımların artırılması”, “faillerin hızlı şekilde tespit edilmesi”, “şikâyet süreçlerinin kolaylaştırılması” ve “anonim hesapların denetlenmesi” gibi öneriler dikkat çekmiştir. “Ceza” kavramı katılımcı cevaplarında **40’ın üzerinde** kez tekrar edilmiş ve en baskın tema olarak öne çıkmıştır.

Katılımcılar, mevcut uygulamalarda mağdurların çoğu zaman hak arama süreçlerini bilmediğini, soruşturmaların uzun sürebildiğini ve özellikle anonim hesaplar üzerinden gerçekleştirilen siber zorbalık eylemlerinde faillerin tespit edilmesinin güçleştiğini ifade etmiştir. Bu durum, yalnızca bireysel mağduriyetleri artırmamakta; aynı zamanda siber zorbalık davranışlarının cezasız kalacağı algısını da güçlendirebilmektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Proje kapsamında elde edilen nicel bulgular da bu ihtiyacı desteklemektedir. Katılımcılar siber zorbalığın ne olduğu konusunda yüksek farkındalığa sahip olmalarına rağmen, dijital haklar ve başvuru mekanizmalarına ilişkin bilgi düzeyinin diğer alanlara kıyasla daha düşük olduğu görülmüştür. Bu bulgu, hukuki düzenlemelerin varlığının tek başına yeterli olmadığını; bu düzenlemelerin gençler tarafından bilinmesini ve etkin biçimde uygulanmasını sağlayacak mekanizmalara ihtiyaç duyulduğunu göstermektedir.

Politika Önerisi

Siber zorbalıkla mücadelede hukuki süreçlerin etkinliğini artırmak amacıyla mevcut mevzuatın uygulama kapasitesi güçlendirilmeli, mağdurların adalete erişimini kolaylaştıracak kurumsal mekanizmalar geliştirilmeli ve dijital platformlarla kamu kurumları arasındaki koordinasyon artırılmalıdır. Hukuki yaptırımların caydırıcılığı artırılırken ifade özgürlüğü, özel hayatın gizliliği ve temel hakların korunması ilkeleri de gözetilmelidir.

Uygulama Adımları

- Siber zorbalık vakalarına ilişkin başvuru süreçleri sadeleştirilmeli ve gençler tarafından kolay erişilebilir hâle getirilmelidir.
- Emniyet birimleri, adli makamlar ve ilgili kurumlara yönelik dijital delil yönetimi ve siber zorbalık konusunda uzmanlaşmış eğitim programları yaygınlaştırılmalıdır.
- Sosyal medya platformları ile yetkili kurumlar arasında hukuka uygun ve hızlı bilgi paylaşımını destekleyen iş birliği mekanizmaları oluşturulmalıdır.
- Üniversitelerde ve kamu kurumlarında dijital haklar ile başvuru yollarını açıklayan rehberler hazırlanmalı ve düzenli olarak güncellenmelidir.
- Anonim ihbar ve danışmanlık mekanizmaları geliştirilerek mağdurların güvenli şekilde destek alması sağlanmalıdır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Beklenen Etki

Bu önerilerin uygulanmasıyla birlikte siber zorbalık vakalarının daha görünür hâle gelmesi, mağdurların hak arama süreçlerine katılımının artması, soruşturma süreçlerinin etkinleşmesi ve hukuki yaptırımların caydırıcılığının güçlenmesi beklenmektedir. Bunun yanı sıra gençlerin dijital haklara ilişkin bilgi düzeyinin artması ve kurumsal mekanizmalara duyulan güvenin güçlenmesi de öngörülmektedir.

5.2 Eğitim ve Farkındalık Faaliyetlerinin Kurumsal Bir Yapıya Kavuşturulması

Sorunun Tanımı

Katılımcıların açık uçlu yanıtlarının tematik analizi sonucunda en fazla tekrar eden ikinci tema, **eğitim ve bilinçlendirme faaliyetlerinin artırılması** olmuştur. Katılımcılar; siber zorbalıkla mücadelenin yalnızca hukuki yaptırımlarla sınırlı kalmaması gerektiğini, uzun vadeli çözümün toplumun tüm kesimlerinde dijital farkındalık kültürünün oluşturulmasıyla mümkün olacağını vurgulamıştır. Özellikle üniversitelerde, ortaöğretim kurumlarında ve gençlik merkezlerinde düzenli eğitimlerin verilmesi gerektiği yönünde çok sayıda öneri sunulmuştur.

Proje kapsamında gerçekleştirilen eğitim faaliyetlerine ilişkin nicel bulgular da bu ihtiyacı desteklemektedir. Katılımcıların büyük çoğunluğu eğitimlerin siber zorbalık konusundaki bilgi düzeylerini artırdığını, sunumların konuyu anlamalarını kolaylaştırdığını ve benzer faaliyetlerin diğer üniversitelerde de uygulanması gerektiğini ifade etmiştir. Bu durum, kısa süreli farkındalık faaliyetlerinin dahi bilgi düzeyi üzerinde anlamlı bir etki oluşturduğunu göstermektedir.

Ancak mevcut uygulamalar incelendiğinde, siber zorbalık eğitimlerinin çoğunlukla proje veya kampanya bazlı gerçekleştirildiği, eğitim kurumlarının standart ve sürdürülebilir eğitim programları içerisinde yeterince yer almadığı görülmektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Bu durum, elde edilen farkındalık kazanımlarının uzun vadede korunmasını güçleştirebilmektedir.

Politika Önerisi

Siber zorbalık, dijital güvenlik, dijital vatandaşlık ve dijital haklar konularını kapsayan eğitim programları, yükseköğretim kurumları başta olmak üzere tüm eğitim kademelerinde sistematik ve sürdürülebilir bir yapıya kavuşturulmalıdır. Eğitimler yalnızca teorik bilgi aktarımına değil; vaka analizleri, senaryo temelli uygulamalar, akran öğrenmesi ve etkileşimli yöntemlere dayalı olarak planlanmalıdır.

Üniversitelerde yeni kayıt yaptıran öğrencilerin oryantasyon programlarına dijital güvenlik modülleri eklenmeli, öğrenci topluluklarının ve gençlik organizasyonlarının bu süreçte aktif rol üstlenmeleri desteklenmelidir.

Uygulama Adımları

- Üniversiteler için ortak bir “Dijital Güvenlik ve Siber Zorbalık Eğitim Modülü” hazırlanmalıdır.
- Oryantasyon programlarında temel dijital güvenlik eğitimi zorunlu hâle getirilmelidir.
- Akademik yıl içerisinde düzenli seminerler, çalıştaylar ve uygulamalı eğitimler gerçekleştirilmelidir.
- Öğrenci toplulukları tarafından yürütülen akran eğitimi modelleri desteklenmelidir.
- Çevrim içi eğitim platformları üzerinden açık erişimli eğitim içerikleri hazırlanmalıdır.
- Eğitim içerikleri düzenli aralıklarla güncellenerek yeni dijital tehditlere uyum sağlamalıdır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Beklenen Etki

Bu önerinin uygulanmasıyla birlikte gençlerin yalnızca siber zorbalığı tanıyan bireyler olmaları değil; dijital ortamda karşılaşılabilecekleri riskleri önceden değerlendirebilen, güvenli dijital davranış geliştirebilen ve karşılaştıkları olaylarda doğru müdahale yöntemlerini uygulayabilen dijital vatandaşlar hâline gelmeleri beklenmektedir. Ayrıca eğitim faaliyetlerinin kurumsallaşması sayesinde proje bazlı çalışmaların etkisinin kalıcı hâle gelmesi ve yükseköğretim kurumlarında ortak bir dijital güvenlik kültürünün oluşması öngörülmektedir.

5.3 Sosyal Medya Platformlarında Önleyici Mekanizmaların Güçlendirilmesi

Sorunun Tanımı

Açık uçlu katılımcı görüşlerinde öne çıkan bir diğer tema, sosyal medya platformlarının siber zorbalıkla mücadelede daha fazla sorumluluk üstlenmesi gerektiğidir. Katılımcılar; özellikle sahte hesaplar, anonim kullanıcılar, hakaret içerikleri, tehdit mesajları ve kişisel verilerin izinsiz paylaşılması gibi durumların dijital platformlarda yeterince hızlı önlenemediğini ifade etmiştir.

Birçok katılımcı, zararlı içeriklerin kaldırılma süreçlerinin uzun sürdüğünü, şikâyet mekanizmalarının kullanıcılar açısından yeterince anlaşılır olmadığını ve bazı durumlarda mağdurların platformlardan etkili geri dönüş alamadığını belirtmiştir. Bunun yanında, anonim hesapların kötüye kullanımını önleyecek doğrulama mekanizmalarının geliştirilmesi gerektiği de sıkça dile getirilen öneriler arasında yer almıştır.

Proje kapsamında yürütülen farkındalık faaliyetleri sonucunda katılımcıların dijital riskleri tanıma düzeylerinin arttığı görülmüş olsa da, bireysel farkındalığın tek başına yeterli olmadığı; dijital platformların güvenli dijital ortam oluşturma sorumluluğunu daha etkin biçimde yerine getirmesi gerektiği anlaşılmaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Politika Önerisi

Sosyal medya platformları; kullanıcı güvenliğini merkeze alan, şeffaf, erişilebilir ve hızlı çalışan içerik denetim sistemlerini güçlendirmeli; siber zorbalık içeriklerinin tespit edilmesi ve kaldırılması süreçlerini daha etkin hâle getirmelidir. Aynı zamanda kullanıcıların hak arama süreçlerini kolaylaştıracak sade ve anlaşılır başvuru mekanizmaları geliştirilmelidir.

Uygulama Adımları

- Şikâyet sistemlerinin kullanıcı dostu şekilde yeniden tasarlanması.
- Tekrarlayan ihlaller için kademeli yaptırım mekanizmalarının uygulanması.
- Yapay zekâ destekli içerik tespit sistemlerinin geliştirilmesi.
- Şeffaflık raporlarında siber zorbalık verilerine düzenli olarak yer verilmesi.
- Genç kullanıcılar için dijital güvenlik bilgilendirme modüllerinin platformlara entegre edilmesi.
- Gerekğinde hukuka uygun şekilde kamu kurumlarıyla koordinasyonun güçlendirilmesi.

Beklenen Etki

Bu önerilerin hayata geçirilmesiyle birlikte zararlı içeriklere müdahale sürelerinin kısılması, mağdurların platformlara olan güveninin artması, tekrar eden siber zorbalık vakalarının azaltılması ve daha güvenli dijital iletişim ortamlarının oluşturulması beklenmektedir. Ayrıca platformların hesap verebilirliğinin güçlenmesi, siber zorbalıkla mücadelede kamu kurumları ve özel sektör arasında daha etkili bir iş birliği sağlayacaktır.

5.4 Üniversitelerde Siber Zorbalık Destek ve Başvuru Mekanizmalarının Güçlendirilmesi

Sorunun Tanımı



**Avrupa Birliği tarafından
finanse edilmektedir**

Katılımcıların açık uçlu yanıtlarının tematik analizi incelendiğinde, siber zorbalığa maruz kalan bireylerin güvenli şekilde destek alabilecekleri kurumsal mekanizmaların oluşturulmasına yönelik taleplerin öne çıktığı görülmektedir. Katılımcılar; mağdurların yaşadıkları olayları çoğu zaman bildirmekten çekindiklerini, hangi kuruma başvuracaklarını bilmediklerini veya başvuru süreçlerinin karmaşık olduğunu ifade etmiştir. Özellikle anonim hesaplar üzerinden gerçekleştirilen hakaret, tehdit, ifşa ve taciz olaylarında mağdurların psikolojik destek ve hukuki danışmanlık hizmetlerine erişimde güçlük yaşayabildiği belirtilmiştir.

Nicel bulgular da bu durumu desteklemektedir. Katılımcılar siber zorbalığın tanımı ve etkileri konusunda yüksek farkındalık düzeyine sahip olmalarına rağmen, dijital haklar ve başvuru mekanizmalarına ilişkin bilgi düzeylerinin görece daha düşük olduğu görülmüştür. Ayrıca katılımcıların önemli bir bölümü mağdurlara nasıl destek olunacağı konusunda daha fazla bilgiye ihtiyaç duyulduğunu ifade etmiştir. Bu durum, siber zorbalıkla mücadelede yalnızca bilinçlendirme faaliyetlerinin yeterli olmadığını; mağdurlara hızlı, güvenilir ve erişilebilir destek sunabilecek kurumsal yapıların da oluşturulması gerektiğini ortaya koymaktadır.

Yükseköğretim kurumlarında psikolojik danışmanlık merkezleri, öğrenci işleri birimleri ve bilgi işlem daireleri gibi çeşitli destek mekanizmaları bulunmasına rağmen, bu yapıların büyük çoğunluğunda siber zorbalığa özgü standart başvuru ve yönlendirme prosedürleri yer almamaktadır. Kurumsal uygulamalar arasındaki farklılıklar ise öğrencilerin hizmetlere erişimini ve süreçlerin etkinliğini olumsuz etkileyebilmektedir.

Politika Önerisi

Yükseköğretim kurumlarında siber zorbalık olaylarının bildirilmesi, değerlendirilmesi ve mağdurlara çok yönlü destek sağlanmasına yönelik kurumsal mekanizmalar oluşturulmalıdır. Bu mekanizmalar yalnızca şikâyet kabul eden bir yapı olarak değil; psikolojik destek, hukuki danışmanlık, dijital güvenlik



**Avrupa Birliği tarafından
finanse edilmektedir**

yönlendirmesi ve gerektiğinde ilgili kamu kurumlarına yönlendirme hizmetlerini bütüncül biçimde sunan koordinasyon birimleri olarak yapılandırılmalıdır.

Ayrıca başvuru süreçlerinin öğrenciler açısından erişilebilir, güvenli ve gizlilik esasına uygun şekilde yürütülmesi sağlanmalı; mağdurların herhangi bir ayrımcılık veya damgalanma endişesi yaşamadan destek alabilecekleri güven ortamı oluşturulmalıdır.

Uygulama Adımları

- Üniversitelerde siber zorbalık başvurularına özel dijital başvuru platformları oluşturulmalıdır.
- Başvuruların gizlilik esasına uygun biçimde değerlendirilmesini sağlayacak standart prosedürler hazırlanmalıdır.
- Psikolojik danışmanlık merkezleri, hukuk danışmanlığı sağlayan birimler ve bilgi işlem daireleri arasında koordinasyon mekanizması kurulmalıdır.
- Öğrencilere yönelik dijital haklar, başvuru yolları ve destek hizmetlerini açıklayan rehberler hazırlanmalı ve düzenli olarak güncellenmelidir.
- Öğrenci toplulukları ve akran destek programları sürece dâhil edilerek mağdurların sosyal destek ağlarına erişimi güçlendirilmelidir.
- Üniversitelerde görev yapan akademik ve idari personele siber zorbalık vakalarının tespiti ve yönlendirilmesine yönelik hizmet içi eğitimler verilmelidir.
- Düzenli aralıklarla anonim memnuniyet ve etkililik değerlendirmeleri yapılarak sistem sürekli iyileştirilmelidir.

Beklenen Etki

Bu önerinin uygulanmasıyla birlikte siber zorbalık mağdurlarının destek hizmetlerine erişiminin kolaylaşması, başvuru oranlarının artması ve olayların erken aşamada tespit edilmesi beklenmektedir. Aynı zamanda öğrencilerin üniversite yönetimine duyduğu güvenin güçlenmesi, psikososyal etkilerin azaltılması ve kurumların siber zorbalıkla mücadelede daha sistematik bir yaklaşım



**Avrupa Birliği tarafından
finanse edilmektedir**

benimsemesi mümkün olacaktır. Uzun vadede ise üniversitelerde güvenli, kapsayıcı ve hak temelli bir dijital kampüs kültürünün gelişmesine katkı sağlayacağı öngörülmektedir.

5.5 Ulusal Düzeyde Kurumsal Koordinasyon ve Çok Paydaşlı İş Birliğinin Güçlendirilmesi

Sorunun Tanımı

Katılımcıların açık uçlu yanıtları incelendiğinde, siber zorbalıkla mücadelenin yalnızca bireysel farkındalık çalışmaları veya tek bir kurumun sorumluluğunda yürütülebilecek bir süreç olmadığı yönünde güçlü bir görüş birliği olduğu görülmektedir. Katılımcılar; eğitim kurumları, kamu kuruluşları, sosyal medya platformları, aileler, sivil toplum kuruluşları ve teknoloji şirketlerinin ortak hareket etmesi gerektiğini sıklıkla ifade etmiştir. Tematik analiz sonucunda “iş birliği”, “ortak çalışma”, “devlet desteği”, “kurumsal koordinasyon” ve “ortak kampanyalar” gibi ifadelerin birçok katılımcı tarafından tekrarlandığı belirlenmiştir.

Proje sürecinde edinilen deneyimler de bu görüşü desteklemektedir. Farklı üniversitelerde gerçekleştirilen eğitim faaliyetleri ve yaygınlaştırma çalışmaları, kurumlar arasında geliştirilen iş birliklerinin proje çıktılarının etki alanını önemli ölçüde artırdığını göstermiştir. Bununla birlikte siber zorbalıkla mücadelede görev ve sorumluluklar farklı kurumlara dağılmış durumdadır. Eğitim faaliyetleri, hukuki süreçler, psikolojik destek hizmetleri, dijital platformların içerik yönetimi ve teknik güvenlik uygulamaları çoğu zaman birbirinden bağımsız yürütülmektedir. Bu durum kaynakların etkin kullanılmasını zorlaştırmakta ve bütüncül politika üretimini sınırlamaktadır.

Uluslararası uygulamalar incelendiğinde ise siber zorbalıkla mücadelede başarılı örneklerin ortak özelliğinin çok paydaşlı yönetim modellerine dayanması olduğu görülmektedir. Eğitim kurumları, düzenleyici otoriteler, teknoloji şirketleri, sivil



**Avrupa Birliği tarafından
finanse edilmektedir**

toplum kuruluşları ve gençlerin karar alma süreçlerine birlikte katıldığı modeller, önleyici politikaların daha etkili uygulanmasına katkı sağlamaktadır.

Politika Önerisi

Siber zorbalıkla mücadelede ulusal düzeyde koordinasyonu sağlayacak, kamu kurumları, yükseköğretim kurumları, yerel yönetimler, sivil toplum kuruluşları, özel sektör ve gençlik temsilcilerinin katılımıyla çalışan sürdürülebilir bir iş birliği modeli oluşturulmalıdır. Bu yapı, yalnızca kriz durumlarında müdahale eden bir mekanizma değil; eğitim, önleme, araştırma, veri paylaşımı ve politika geliştirme süreçlerini birlikte yürüten sürekli bir koordinasyon platformu olarak tasarlanmalıdır.

Politika geliştirme süreçlerinde gençlerin yalnızca hedef grup olarak değil, karar alma süreçlerine aktif katkı sunan paydaşlar olarak yer almaları sağlanmalıdır. Gençlik odaklı projelerden elde edilen deneyim ve geri bildirimler, ulusal politika belgelerinin hazırlanmasında sistematik biçimde değerlendirilmelidir.

Uygulama Adımları

- İlgili kamu kurumlarının koordinasyonunda **Ulusal Siber Zorbalıkla Mücadele Çalışma Grubu** oluşturulmalıdır.
- Yükseköğretim kurumları arasında iyi uygulama örneklerinin paylaşılacağı ortak bir iş birliği ağı kurulmalıdır.
- Gençlik projeleri kapsamında geliştirilen eğitim materyalleri ve politika önerileri ortak bir dijital platformda toplanarak kamuoyunun erişimine açılmalıdır.
- Düzenli aralıklarla ulusal çalıştaylar, politika forumları ve gençlik zirveleri düzenlenmelidir.
- Kamu kurumları ile sosyal medya platformları arasında kullanıcı güvenliğini geliştirmeye yönelik iş birliği mekanizmaları güçlendirilmelidir.



**Avrupa Birliği tarafından
finanse edilmektedir**

- Üniversiteler ve araştırma merkezleri tarafından yürütülen bilimsel çalışmalar desteklenmeli; siber zorbalığa ilişkin ulusal veri üretimi teşvik edilmelidir.
- Politika geliştirme süreçlerine gençlik temsilcileri, öğrenci toplulukları ve sivil toplum kuruluşlarının katılımı kurumsal güvence altına alınmalıdır.

Beklenen Etki

Bu önerinin hayata geçirilmesiyle birlikte siber zorbalıkla mücadelede kurumlar arası koordinasyonun güçlenmesi, kaynakların daha etkin kullanılması ve ulusal ölçekte ortak bir politika yaklaşımının geliştirilmesi beklenmektedir. Ayrıca gençlerin politika geliştirme süreçlerine katılımının artması, alınacak kararların hedef kitlenin ihtiyaçlarına daha duyarlı olmasını sağlayacaktır. Kurumsal iş birliğinin güçlenmesi; eğitim, önleme, erken müdahale ve mağdur destek hizmetlerinin birbirini tamamlayan bir sistem içerisinde yürütülmesine katkı sunacak, böylece siber zorbalıkla mücadelede sürdürülebilir ve bütüncül bir yönetim modeli oluşturulacaktır.

5.6 Sosyal Medya Platformlarında Hesap Verebilirlik ve Güvenli Dijital Ortamların Güçlendirilmesi

Sorunun Tanımı

Proje kapsamında gerçekleştirilen açık uçlu anket sorularının içerik analizi sonucunda katılımcılar tarafından sıklıkla dile getirilen konulardan biri, sosyal medya platformlarının siber zorbalıkla mücadelede daha etkin sorumluluk üstlenmesi gerektiğidir. Katılımcılar özellikle anonim hesaplar aracılığıyla gerçekleştirilen hakaret, tehdit, ifşa, nefret söylemi ve çevrimiçi taciz davranışlarının önlenmesinde mevcut platform politikalarının her zaman yeterli olmadığını ifade etmiştir. Bunun yanında şikâyet süreçlerinin uzun sürmesi, kullanıcıların geri bildirim mekanizmaları hakkında yeterince bilgilendirilmemesi



**Avrupa Birliği tarafından
finanse edilmektedir**

ve zararlı içeriklerin platformlarda uzun süre erişilebilir kalabilmesi de dikkat çekilen başlıca sorun alanları arasında yer almıştır.

Proje kapsamında gerçekleştirilen eğitim faaliyetleri sonucunda katılımcıların dijital riskleri tanıma düzeylerinde önemli artış gözlenmiş olmasına rağmen, bireysel farkındalığın tek başına güvenli dijital ortamların oluşturulması için yeterli olmadığı görülmektedir. Dijital platformlar, milyonlarca kullanıcıyı aynı ortamda buluşturan yapıları nedeniyle siber zorbalığın önlenmesinde önemli bir sorumluluğa sahiptir. Bu nedenle platformların yalnızca kullanıcı şikâyetlerine yanıt veren pasif yapılar olmaktan çıkarak riskleri önceden tespit eden, kullanıcı güvenliğini önceleyen ve hesap verebilir uygulamalar geliştiren aktif paydaşlar hâline gelmeleri gerekmektedir.

Uluslararası uygulamalar incelendiğinde Avrupa Birliği'nin **Dijital Hizmetler Yasası (Digital Services Act)** gibi düzenlemelerle çevrimiçi platformların kullanıcı güvenliği, şeffaflık ve içerik yönetimi konularındaki sorumluluklarını artırmaya yönelik önemli adımlar attığı görülmektedir. Türkiye'de de benzer şekilde kullanıcı haklarını koruyan, şeffaflığı güçlendiren ve platformların hesap verebilirliğini artıran uygulamaların geliştirilmesi önem taşımaktadır.

Politika Önerisi

Sosyal medya platformları; kullanıcı güvenliğini esas alan, şeffaf, hızlı ve erişilebilir içerik yönetim sistemlerini güçlendirmeli; siber zorbalık içeriklerinin tespiti, değerlendirilmesi ve kaldırılmasına yönelik süreçlerde hesap verebilir uygulamaları yaygınlaştırmalıdır. Aynı zamanda genç kullanıcıların güvenli dijital davranış geliştirmelerini destekleyen bilgilendirme ve eğitim araçları platformların temel hizmetlerinin bir parçası hâline getirilmelidir.

Uygulama Adımları

- Siber zorbalık bildirim süreçleri sadeleştirilmeli ve kullanıcı dostu hâle getirilmelidir.



**Avrupa Birliği tarafından
finanse edilmektedir**

- Zararlı içeriklerin değerlendirilme süreleri için şeffaf performans kriterleri belirlenmelidir.
- Tekrarlayan ihlallerde kademeli yaptırım mekanizmaları uygulanmalıdır.
- Yapay zekâ destekli içerik tespit sistemleri insan denetimiyle birlikte geliştirilmelidir.
- Genç kullanıcılar için güvenli internet kullanımına ilişkin yönlendirici dijital modüller oluşturulmalıdır.
- Platformlar düzenli şeffaflık raporları yayımlayarak siber zorbalık başvuruları ve alınan önlemler hakkında kamuoyunu bilgilendirmelidir.
- Kamu kurumları ve akademik kuruluşlarla ortak bilinçlendirme kampanyaları yürütülmelidir.

Beklenen Etki

Bu önerilerin uygulanmasıyla birlikte zararlı içeriklere müdahale sürelerinin kısılması, kullanıcıların platformlara duyduğu güvenin artması, siber zorbalık vakalarının tekrar oranlarının azaltılması ve güvenli dijital iletişim kültürünün güçlenmesi beklenmektedir. Ayrıca sosyal medya platformlarının hesap verebilirliğinin artması, kamu kurumları ile dijital platformlar arasında daha etkili bir iş birliği ortamı oluşturacaktır.

5.7 Sürekli İzleme, Araştırma ve Veri Temelli Politika Geliştirme Mekanizmalarının Oluşturulması

Sorunun Tanımı

Proje sürecinde elde edilen bulgular, siber zorbalığın teknolojik gelişmelerle birlikte sürekli değişen ve yeni biçimler kazanan dinamik bir sorun olduğunu ortaya koymuştur. Yapay zekâ destekli içerik üretimi, geçici içerikler, anonim iletişim araçları ve yeni nesil dijital platformlar, siber zorbalığın yöntemlerini ve yayılma biçimlerini sürekli değiştirmektedir. Bu nedenle belirli dönemlerde



**Avrupa Birliği tarafından
finanse edilmektedir**

hazırlanan politika belgelerinin tek başına uzun vadeli çözümler üretmesi mümkün değildir.

Katılımcıların açık uçlu yanıtlarında da yalnızca mevcut sorunlara müdahale edilmesinin yeterli olmayacağı; düzenli araştırmalar yapılması, gençlerin görüşlerinin sürekli alınması ve geliştirilen politikaların belirli aralıklarla gözden geçirilmesi gerektiği yönünde değerlendirmeler yer almıştır. Proje kapsamında gerçekleştirilen anket çalışması, gençlerin görüşlerinin politika geliştirme süreçlerine doğrudan katkı sağlayabileceğini göstermiştir.

Bununla birlikte Türkiye’de siber zorbalığa ilişkin düzenli, karşılaştırılabilir ve ulusal ölçekte sürdürülen veri üretiminin sınırlı olması, politika yapıcıların karar alma süreçlerinde güncel ve kapsamlı verilere erişimini güçleştirebilmektedir. Düzenli veri üretimi ve etki değerlendirmesi yapılmadığı sürece geliştirilen politikaların başarısını ölçmek ve yeni ihtiyaç alanlarını belirlemek zorlaşmaktadır.

Politika Önerisi

Siber zorbalıkla mücadelede ulusal düzeyde sürdürülebilir bir izleme ve değerlendirme sistemi oluşturulmalıdır. Politika geliştirme süreçleri düzenli araştırmalar, akademik çalışmalar, gençlerin geri bildirimleri ve kurumsal veriler ışığında güncellenmeli; tüm paydaşların katkı sağlayabileceği kanıta dayalı bir yönetim modeli benimsenmelidir.

Uygulama Adımları

- Ulusal ölçekte düzenli siber zorbalık araştırmaları gerçekleştirilmelidir.
- Üniversitelerde yıllık dijital güvenlik ve siber zorbalık değerlendirme raporları hazırlanmalıdır.
- Gençlik projelerinde elde edilen verilerin anonimleştirilerek politika geliştirme süreçlerinde kullanılması sağlanmalıdır.
- Kamu kurumları, üniversiteler ve araştırma merkezleri arasında ortak veri paylaşım mekanizmaları oluşturulmalıdır.



**Avrupa Birliği tarafından
finanse edilmektedir**

- Geliştirilen politikaların etkililiğini değerlendirmek amacıyla performans göstergeleri belirlenmeli ve düzenli izleme raporları yayımlanmalıdır.
- Gençlerin politika geliştirme süreçlerine katılımını sağlayacak dijital görüş ve öneri platformları oluşturulmalıdır.
- Yeni teknolojilerin ortaya çıkardığı risklere yönelik araştırma fonları ve disiplinler arası bilimsel çalışmalar desteklenmelidir.

Beklenen Etki

Bu önerinin uygulanmasıyla birlikte siber zorbalığa ilişkin karar alma süreçlerinin güncel verilerle desteklenmesi, geliştirilen politikaların etkililiğinin düzenli olarak ölçülmesi ve değişen dijital risklere daha hızlı uyum sağlanması mümkün olacaktır. Ayrıca gençlerin deneyim ve beklentilerinin politika üretim süreçlerine sistematik biçimde dâhil edilmesi, geliştirilecek uygulamaların hedef kitlenin gerçek ihtiyaçlarına daha uygun olmasına katkı sağlayacaktır. Kanıta dayalı yönetim anlayışının güçlenmesi, siber zorbalıkla mücadelede sürdürülebilir, hesap verebilir ve etkili kamu politikalarının oluşturulmasına önemli katkılar sunacaktır.



**Avrupa Birliği tarafından
finanse edilmektedir**

6. Sonuç ve Değerlendirme

Dijital teknolojilerin bireylerin eğitim, iletişim ve sosyal yaşamındaki rolünün her geçen gün artması, siber zorbalığı yalnızca bireysel bir davranış problemi olmaktan çıkararak toplumsal, hukuki, psikolojik ve teknolojik boyutları bulunan çok yönlü bir politika alanına dönüştürmüştür. Özellikle gençlerin dijital ortamlarda daha fazla zaman geçirmesi, güvenli dijital ortamların oluşturulmasını ve siber zorbalığın önlenmesine yönelik sürdürülebilir politikaların geliştirilmesini zorunlu hâle getirmektedir.

Avrupa Dayanışma Programı (European Solidarity Corps – ESC30-SOL) kapsamında yürütülen **Siber Zorbalığa Karşı Gençlik İttifakı** projesi, bu ihtiyaçtan hareketle gençlerin dijital güvenlik konusundaki bilgi ve farkındalık düzeylerini artırmayı, güvenli dijital davranışları teşvik etmeyi ve siber zorbalıkla mücadelede gençlerin aktif katılımını desteklemeyi amaçlamıştır. Proje süresince gerçekleştirilen eğitim faaliyetleri, seminerler, farkındalık kampanyaları, kamu spotları, dijital içerikler ve yaygınlaştırma çalışmaları sayesinde farklı üniversitelerden çok sayıda gence ulaşılmış, siber zorbalık konusunda önemli öğrenme çıktıları elde edilmiştir.

Bu rapor kapsamında değerlendirilen anket bulguları, katılımcıların siber zorbalığın tanımı, dijital güvenlik ve güvenli internet kullanımı konularında yüksek düzeyde farkındalık geliştirdiğini göstermektedir. Bununla birlikte dijital haklar, başvuru mekanizmaları ve mağdurlara yönelik kurumsal destek süreçlerine ilişkin bilgi düzeyinin diğer alanlara kıyasla daha düşük olduğu belirlenmiştir. Açık uçlu



**Avrupa Birliği tarafından
finanse edilmektedir**

soruların tematik analizi ise katılımcıların hukuki yaptırımların güçlendirilmesi, eğitim faaliyetlerinin yaygınlaştırılması, sosyal medya platformlarının daha fazla sorumluluk üstlenmesi, güvenli başvuru mekanizmalarının oluşturulması ve kurumlar arası iş birliğinin geliştirilmesi yönünde ortak beklentilere sahip olduğunu ortaya koymuştur.

Bu doğrultuda raporda sunulan politika önerileri; proje kapsamında elde edilen nicel ve nitel bulgular, katılımcı görüşleri ve ulusal ile uluslararası iyi uygulama örnekleri birlikte değerlendirilerek hazırlanmıştır. Öneriler; üniversiteler, kamu kurumları, yerel yönetimler, sosyal medya platformları, sivil toplum kuruluşları ve diğer ilgili paydaşların ortak sorumluluk anlayışıyla hareket etmesini esas alan bütüncül bir yaklaşım sunmaktadır.

Proje sürecinde geliştirilen katılımcı model, gençlerin yalnızca politika uygulamalarının hedef kitlesi değil, aynı zamanda politika geliştirme süreçlerinin aktif paydaşları olabileceğini göstermiştir. Gençlerin deneyimlerinin, ihtiyaçlarının ve çözüm önerilerinin karar alma mekanizmalarına dâhil edilmesi, geliştirilecek politikaların uygulanabilirliğini ve toplumsal kabulünü artıracaktır.

6.1 Dijital Şiddet ve Türkiye’de Durum

Dünya genelinde kadınların yaklaşık %73’ü internet üzerinden tacize uğradığını bildirmektedir ve çevrimiçi vakit geçiren kadınların %85’i dijital şiddete tanık olmaktadır (UN Women, 2023). Türkiye özelinde ise her beş kişiden biri dijital şiddete maruz kalmakta; kadınların %51’i yazılı, sesli veya görüntülü taciz mesajları almakta, %46’sı ise ısrarlı takip ile karşı karşıya kalmaktadır (Ekmek ve



**Avrupa Birliği tarafından
finanse edilmektedir**

Gül, 2022). Bu şiddet eylemleri çoğunlukla Instagram (%53), Facebook (%35) ve Twitter (%19) üzerinden gerçekleşmekte olup, failler genellikle tanımadıkları kişiler, troller veya eski partnerler, akrabalar ve arkadaşlar olmaktadır (Ekmek ve Gül, 2022). Dijital şiddetin türleri arasında taciz mesajları, hakaret veya tehdit içerikli yorumlar, özel içeriklerin rızasız paylaşılması, şantaj ve hesaplara izinsiz erişim gibi eylemler öne çıkmaktadır (UN Women, 2023; Yılmaz & Demir, 2024).

6.2 Geleceğe Yönelik Perspektif

Dijital teknolojilerde yaşanan hızlı gelişmeler, siber zorbalığın yöntemlerini ve etkilerini sürekli değiştirmektedir. Yapay zekâ destekli içerik üretimi, derin sahte (deepfake) teknolojileri, artırılmış gerçeklik uygulamaları, yeni nesil sosyal medya platformları ve dijital iletişim araçları, gelecekte siber zorbalığın daha karmaşık biçimlerde ortaya çıkabileceğini göstermektedir. Bu nedenle geliştirilecek politikaların statik değil, değişen teknolojik koşullara uyum sağlayabilecek dinamik bir yapıya sahip olması gerekmektedir.

Gelecekte yürütülecek çalışmaların farklı yaş gruplarını, eğitim kademelerini ve toplumsal kesimleri kapsayacak şekilde genişletilmesi; boylamsal araştırmalarla politika uygulamalarının uzun dönemli etkilerinin değerlendirilmesi önem taşımaktadır. Ayrıca yapay zekâ, büyük veri analitiği ve dijital davranış analizlerinden yararlanılarak siber zorbalığın erken tespitine yönelik yenilikçi araştırmaların desteklenmesi, bu alandaki politika geliştirme süreçlerine önemli katkılar sağlayacaktır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Siber zorbalıkla mücadelede başarı, yalnızca hukuki düzenlemeler veya teknolojik çözümlerle değil; eğitim, farkındalık, dijital vatandaşlık bilinci ve kurumlar arası güçlü iş birliğiyle mümkün olacaktır. Gençlerin aktif katılımını merkeze alan, bilimsel verilerle desteklenen ve düzenli olarak güncellenen politikalar, güvenli dijital ortamların oluşturulmasında temel unsur olacaktır.

Sonuç olarak **Siber Zorbalığa Karşı Gençlik İttifakı** projesi, gençlerin görüşlerini merkeze alan katılımcı yaklaşımı, disiplinler arası çalışma modeli ve kanıta dayalı politika önerileriyle yalnızca bir farkındalık projesi olmanın ötesine geçmiş; siber zorbalıkla mücadelede sürdürülebilir kamu politikalarının geliştirilmesine katkı sunan örnek bir gençlik girişimi ortaya koymuştur. Bu raporda sunulan önerilerin ilgili kurum ve kuruluşlar tarafından değerlendirilmesi ve uygulamaya aktarılması, Türkiye’de daha güvenli, kapsayıcı ve bilinçli bir dijital toplumun oluşturulmasına katkı sağlayacaktır.



**Avrupa Birliği tarafından
finanse edilmektedir**

7. Yararlanılan Kaynaklar

Uluslararası Kuruluşlar

- European Commission. *European Solidarity Corps Programme Guide*.
- European Union Agency for Cybersecurity (ENISA). *Cybersecurity Education and Awareness Resources*.
- UNESCO. *Behind the Numbers: Ending School Violence and Bullying*.
- UNICEF. *Cyberbullying: What is it and how to stop it?*
- OECD. *Digital Education Outlook*.

Ulusal Kaynaklar

- Bilgi Teknolojileri ve İletişim Kurumu (BTK). *Güvenli İnternet Merkezi Yayınları*.
- Kişisel Verileri Koruma Kurumu (KVKK). *Kişisel Verilerin Korunmasına İlişkin Rehberler*.
- T.C. Adalet Bakanlığı. İlgili mevzuat.
- Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı yayınları.

Bilimsel Yayınlar

- Siber zorbalık, dijital vatandaşlık ve dijital güvenlik alanındaki güncel ulusal ve uluslararası akademik çalışmalar.



**Avrupa Birliği tarafından
finanse edilmektedir**

8. Teşekkür

Bu politika önerileri raporu, Avrupa Dayanışma Programı (European Solidarity Corps – ESC30-SOL) kapsamında yürütülen **Siber Zorbalığa Karşı Gençlik İttifakı** projesinin bir çıktısı olarak hazırlanmıştır.

Projenin planlanması, uygulanması ve bu raporun hazırlanması sürecinde desteklerini esirgemeyen başta **Türkiye Ulusal Ajansına** ve **Sakarya Üniversitesine** teşekkür ederiz.

Proje süresince değerli rehberliği ve katkılarıyla bizlere yol gösteren **Proje Koçu Öğr. Gör. Dr. Sadık Demirbağ’a**, politika önerilerinin geliştirilmesi sürecindeki akademik katkıları ve mentörlüğü için **Dr. Öğr. Üyesi Hatice Turut Demirbağ’a** teşekkürlerimizi sunarız.

Ayrıca proje faaliyetlerine katılarak bilgi, deneyim ve görüşlerini paylaşan tüm katılımcılara, farkındalık çalışmalarına destek veren paydaş kurum ve kuruluşlara, gönüllülük anlayışıyla emek veren proje ekibine ve gençlik çalışmalarına katkı sağlayan herkese teşekkür ederiz.

Bu raporda yer alan politika önerileri, gençlerin görüşleri ve proje sürecinde elde edilen deneyimler doğrultusunda hazırlanmış olup, güvenli ve kapsayıcı dijital ortamların oluşturulmasına katkı sunması temennisiyle kamuoyu ve ilgili paydaşların değerlendirmesine sunulmaktadır.

Siber Zorbalığa Karşı Gençlik İttifakı Proje Ekibi



**Avrupa Birliği tarafından
finanse edilmektedir**



**Avrupa Birliđi tarafından
finanse edilmektedir**



**Avrupa Birliđi tarafından
finanse edilmektedir**



Siber Zorbalığa Karşı Gençlik İttifakı



Avrupa Birliği tarafından
finanse edilmektedir



2024-3-TR01-ESC30-SOL-000284071

"Avrupa Dayanışma Programı kapsamında Avrupa Birliği tarafından desteklenmektedir. Bu raporda yer alan görüş, değerlendirme ve öneriler yalnızca yazarlarına aittir. Avrupa Komisyonu ve Türkiye Ulusal Ajansı, bu yayında yer alan bilgilerin kullanımından veya içerdiği görüşlerden sorumlu tutulamaz."



**Avrupa Birliği tarafından
finanse edilmektedir**